Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On Certain Ternary Cubic-Form Equations.

BY J. J. SYLVESTER.

CHAPTER I.

EXCURSUS C. — ON THE TRISECTION AND QUARTISECTION OF THE ROOTS OF UNITY TO A PRIME-NUMBER INDEX.

WHAT follows, so far as it relates to the trisection of the primitive roots of unity, may be regarded as auxiliary to Postscriptum 2, Vol. II. of this Journal, p. 387, inasmuch as it establishes the equation in ω which, when $x = \frac{\omega - 1}{3}$, becomes the equation assumed in line 4, p. 388. The rest is episodical, except so far as it may be regarded as correlative to the subject matter of Titles 1 and 2 of Excursus A.*

It will be seen that the equations to a system of three and four periods, usually obtained by long and tedious processes, may, with the aid of one simple and well-known principle, be deduced by processes almost elementary in their character, and into which enter no algebraical calculations except of the very easiest kind.

A sketch of the method was laid by me before the Scientific Congress held at Rheims in the month of August last.

The index p of the roots is, as usual, supposed to be a prime number; e is the number of the periods, f the number of roots whose sum forms a period, so that $ef = p - 1$; the periods themselves will be called η, viz. $\eta_1, \eta_2, \ldots . \eta_e$.

Preliminaries.

1. I say, in the first place, that the sum of the i^{th} powers of the periods will be congruous to $-f^{i-1}$ in respect to the modulus p.

---

* In any future redistribution of the contents of the entire memoir, it would be proper to incorporate the matter contained in Proscriptum 2, pp. 387-389, with this Excursus.

For, were it not that in the development of the i^{th} power of any one of the η's some of the combinations of the powers of the roots were unity, it is obvious that we should have $\Sigma\,\eta^i = -\,ef^i \div (p-1)$, i. e. $-f^{i-1}$, and that we might regard every term in such development as equivalent to $-\frac{1}{p-1}$, without affecting this result. The existence of terms equal to unity will render it necessary to substitute for any such term 1 instead of $-\frac{1}{p-1}$, in order to obtain a correct result, and if there be N of them, the correction to be introduced will be $N\left(1+\frac{1}{p-1}\right)$, i. e. $\frac{N}{p-1}\cdot p$; but as it is obvious that the result must be an integer, it follows that N must be double by $(p-1)$, and consequently the value of $\Sigma\,\eta^i$ *to modulus p* will be $-f^{i-1}$, i. e. $-\left(\frac{p-1}{e}\right)^{i-1}$, as was to be shown.

2. From the above it follows that *to modulus p*,

$$\Sigma\,(e\eta+1)^i \equiv (-1)^i + e(-1)^{i-1} + e\,\frac{e-1}{2}\,(-1)^{i-2} +, \text{etc.}, \equiv (-1+1)^e \equiv 0,$$

or, in other words, $\Sigma\,(e\eta+1)^i$ is divisible by p.

But, if s_i and σ_i represent, respectively, the sum of the i^{ary} combinations and i^{ary} powers of the roots of an equation, we know that $(-)^i s_i =$ coefficient of x^i in $e^{-\sigma_1 x - \frac{\sigma_2}{2}x^2 - \frac{\sigma_3}{3}x^3 \cdots}$, so that s_i multiplied by numbers none exceeding i, is expressible as the sum of integer multiples of $\sigma_\lambda \sigma_\mu \sigma_\nu \ldots.$ where $\lambda + \mu + \nu + \ldots. = i$.

3. Consequently, s_i multiplied by integers none greater than i, when the roots in question are the e values of $e\eta + 1$ and $i > 0$, will be divisible by p, and consequently, since e is less than p, all the coefficients of the equation to which those roots appertain will be divisible by p, the first, of course (which is unity), excepted.

Since $\Sigma\,(e\eta+1) = e\Sigma\eta + e = 0$, the equation whose roots are $\omega_1, \omega_2, \ldots. \omega_e$ where $\omega = e\eta + 1$ will be of the form $\omega^e + P\omega^{e-2} + Q\omega^{e-3} +$, etc., where P, Q, etc., each contain p; and I may remark, incidentally (although the fact is immaterial to the object in view), that, as may easily be seen, $\Sigma\omega^i$ will be divisible not only by p but also by e, and that consequently the coefficient of ω^{e-i}, in the above equation, will contain the greatest common divisor to e and i.

4. The coefficient P has one or the other of two determinate algebraical values according as f, i. e. $\frac{p-}{e}$, is even or odd.

In the former case, the congruence $x^e + 1 \equiv 0$ [mod p] is soluble, and in the latter, insoluble. Accordingly, in the latter case, we shall have $\Sigma\eta^2 = -f$, and in the former $\Sigma\eta^2 = p - f$, and in each case $\Sigma\eta^2$ will be an odd number. Also, when f is odd (which involves the necessity of e being even) $\Sigma\omega^2 = \Sigma\,(e\eta + 1)^2 = -\,e^2\frac{p-1}{e} - 2e + e = -\,ep$, and when f is even $\Sigma\omega^2$ will be this result augmented by e^2p, i. e. $(e^2 - e)p$.

Consequently, $P = \frac{e}{2}p$, or $= -\frac{e^2-e}{2}p$, according as f is odd or even.

Thus, when $e = 3$, f being necessarily even, $P = -\,3p$, and when $e = 4$, $P = -\,6p$, or $= 2p$, according as $\frac{p-1}{4}$ is even or odd.*

5. With regard to what immediately follows it will also be necessary to determine the *form* of Q in respect to certain moduli for the cases of e equal to 3 and e equal to 4. In the former case $\Sigma\omega^3 = \Sigma\,(e\eta + 1)^3 = \Sigma\,(e^3\eta^3 + 3\,e^2\eta^2 + 3\,e\eta + 1) \equiv 3 \bmod 9$, and consequently, since $Q = -\,\frac{1}{3}\,\Sigma\omega^3$, $-\,3\,Q \equiv 3 \bmod 9$ and $-\,Q \equiv 1 \bmod 3$.

In the latter case, i. e. when $e = 4$, since $\Sigma\eta^2$ is always odd $\Sigma\omega^3$ [to mod 32] $\equiv 16 - 12 + 4$, i. e. $\equiv 8$, and, consequently, $-\,3\,Q \equiv 8$ to that modulus.

These *preliminaries* being established, I will now proceed to state the principle referred to in the exordium.

Principle.

A rational integer function of any set of periods of the roots of unity whose coefficients are all whole numbers, which does not change its value for a circular substitution executed upon the periods, it is well known, must be an integer number; but to this I add that if such function, without changing its arithmetical value, undergoes a change of sign when such a substitution is made, it must necessarily be an integer number multiplied by the difference of the two periods into which the entire sum of the roots may be divided, that is to say, will be a multiple of $\sqrt{p}$, when p is of the form $4\,K + 1$ and of $\sqrt{-p}$, when p is of the form $4\,K - 1$.†

As an example, the product of the differences of the roots of the equation in η will be an integer number when e, the number of the periods, is odd and an integer number multiple of $\sqrt{p}$ or $\sqrt{-p}$ (according as $\frac{p-1}{2}$ is even or odd), when the number of periods is even. As another example, if $e = 2\,\epsilon$, the function

$$(\eta_0 - \eta_\epsilon)\,(\eta_1 - \eta_{\epsilon+1})\,(\eta_2 - \eta_{\epsilon+2}) \,\ldots\ldots\, (\eta_{\epsilon-1} - \eta_{2\epsilon-1})$$

---

* When $e = 2$, $P = p$ or $-p$ according as f is odd or even, so that the equation in ω takes the known form $\omega^2 \pm p = 0$.

† To put the matter more clearly, call the alternating function F and the difference spoken of Δ. Then ΔF is invariable in sign as well as in magnitude for the circular substitutions in question. Hence $F = \frac{\text{An Integer}}{\sqrt{\pm p}}$ but F^2 is an Integer; therefore $F =$ An Integer $\sqrt{\pm\,p}$. Q. E. D.

which changes its sign but not its quantitative value, when $0, 1, 2, 3, \ldots (2\epsilon - 1)$ are replaced by $1, 2, 3, \ldots -1, 0$ will be an integer multiple of $\sqrt{p}$, or of $\sqrt{-p}$, according as ϵ is even or odd.

We are now in a position to obtain without difficulty the well-known equivalent to the equation corresponding to $e = 3$, given at p. 388, and the corresponding pair of equations for the case of $e = 4$.

A. *Case of* $e = 3$.

The equation in ω, from what has been shown in the preliminaries, must be of the form $\omega^3 - 3px + pq = 0$, and it only remains to determine q.

The discriminant of the above equation being $q^2p^2 - 4p^3$, it follows that the product of the differences of its roots will be $27(4p^3 - q^2p^2)$. But this product is 3^6 into $(\eta_0 - \eta_1)^2 (\eta_0 - \eta_2)^2 (\eta_1 - \eta_2)^2$, which latter, by the *principle*, is of the form M^2. We have, therefore,

$$4p^3 - q^2p^2 = 27M^2 = 27m^2p^2.$$

Hence,
$$4p = q^2 + 27m^2,$$

which serves to determine the value of q^2 absolutely.

To find the value of q, it follows from the preliminaries that $qp \equiv -1 \bmod 3$, and, consequently, since $p \equiv 1 \bmod 3$, $q \equiv -1 \bmod 3$, so that q is perfectly determined.

B. *Case of* $e = 4$.

$\omega^2 - 2\sqrt{p}\omega + R = 0$, $\omega^2 + 2\sqrt{p}\omega + R' = 0$, will be the form of the equations containing, respectively, the pairs of roots ω_0, ω_2 and ω_1, ω_3; for

$$\omega_0 + \omega_2 = (4\eta_0 + 1) + (4\eta_2 + 1) = 2(2\overline{\eta_0 + \eta_2} + 1) = 2(2\delta_0 + 1),$$

and, similarly, $\omega_1 + \omega_3 = 2(2\overline{\eta_1 + \eta_3} + 1) = 2(2\delta_1 + 1)$ where δ_0 and δ_1 are the two periods which make up together the sum of all the roots, so that $2\delta_0 + 1$ and $2\delta_1 + 1$ are the roots of the equation $\Omega^2 - p = 0$, the sign of the last term being fixed from the fact of $\frac{p-1}{2}$ being by hypothesis even.

Furthermore, R, R' must be of the form $Ap + B\sqrt{p}, Ap - B\sqrt{p}$; for $(R - R')\sqrt{p}$, being integer, requires that R, R' shall be of the form $A_1 + B\sqrt{p}$, $A_1 - B\sqrt{p}$, and then RR' being an integer multiple of p involves the necessity of A_1^2, and therefore of A_1 containing p.

The product $(\eta_0 - \eta_2)(\eta_1 - \eta_3)$ consequently becomes

$$((A - 1)p + B\sqrt{p})\ ((A - 1)p - B\sqrt{p}),$$

which by the principle must be of the form m^2p, and consequently,

$$(A-1)^2p-B^2=C^2 \text{ or } (A-1)^2p=B^2+C^2.$$

The coefficient of ω^2 becomes $-4p+2Ap$ which, by the preliminaries, when $\frac{p-1}{4}$ is even must be equal to $-6p$, so that $A=-1$, and when $\frac{p-1}{4}$ is odd must be equal to $2p$, so that $A=3$.

In each case, therefore, $(A-1)^2=4$ and $4p=B^2+C^2$; consequently, if $p=g^2+h^2$, $4g^2=B^2$, and $4h^2=C$, and the complete equation in ω containing the roots $\omega_0, \omega_1, \omega_2, \omega_3$, becomes $(\omega^2-p)^2-4p(\omega+g)^2=0$ when $\frac{p-1}{4}$ is even and $(\omega^2+3p)^2-4p(\omega+g)^2=0$ when $\frac{p-1}{4}$ is odd. In either case g^2 is given, but the sign of g requires to be determined; alike, however, for one case as for the other, $-8pg$ being the 3d coefficient after the first, we must have, as shown in the preliminaries, $24pg\equiv 8$ [mod 32], and consequently, since p is of the form $4K+1$, $24g\equiv 8$ [mod 32]. Hence, $3g\equiv 1$ [mod 4], i. e. $g\equiv -1$ [mod 4], which gives the required complete determination of g.

The quartisecting equations thus naturally arrived at are expressed in the form in which, according to Bachmann (Kreistheilung, p. 230), they were first presented by Lebesgue; the method here given for finding the equations for the trisection and quatrisection of the roots of unity will be found on examination to be incomparably simpler, shorter, and more direct than any in common use, and as removing a serious stumbling-block from the path of the student, and, occurring, so far as regards trisection, in the natural course of the development of my subject, I have thought entitled to a place in this memoir. Why I require the trisecting equation is, as will be remembered, to enable me to obtain the conditions of 2 and of 3 being cubic residues to a given index. The condition for 2 being such, strange to say, is nowhere to be found in Bachmann's Kreistheilung, although the cubic character of 3 is there duly and fully made out.

The conditions of the one and of the other being cubic residues were, I am informed by M. Lucas, given for the first time in a letter from Gauss to Mlle. Sophie Germain.

EXCURSUS B.

TITLE 5 (*bis*).— *On the Law of Squares.*

There being errors and inaccuracies not a few in the matter printed under this title, owing to my absence abroad as it went through the press, I have thought it desirable to rewrite it, rectifying the errors, and supplying some steps which were wanting in the demonstrations.* I shall, in what follows, use through-out P_i to denote the i^{th} derivative of P, and x_i, y_i, z_i to signify the reduced co-ordinates of P_i, so that P_1, x_1, y_1, z_1 will mean the same as P, x, y, z respectively. $x + y = 0$, $z = 0$ will be taken as the auxiliary point of inflexion, serving to complete the scale, and will be called I. In the natural scale it is easy to see that any derived co-ordinate, as z_i, must contain the original one, as z. For when $z = 0$, P will be a point of inflexion and P_i identical with P, hence (x_i, y_i, z_i) will express the same point of inflexion, and consequently $z_i = 0$; hence z_i must contain z. When we leave the rational scale, so that i is a multiple of 3, z must contain xyz. For when $z = 0$, the i^{th} derivative P will be one of the three points I, I', I'', expressed by $z = 0$, $x^3 + y^3 = 0$. If P is I, P_3 is obviously I; if P is I', P_2 is I', and P_3 will be the connective of P_2 and I''; consequently P_3 is I and $z = 0$, and the same will be the case if P is I''; hence z'_3 contains z.

---

* In the postscript which was thought out on board the transatlantic steamer, the Bothnia, and written out, as far as I can recollect, at a single sitting a day or two before posting it at Queenstown, I have not been able to detect any inaccuracy in the results, although some additional steps and explanations might advantageously have been supplied.

There is, perhaps, one slight exception to be made to this statement as regards the very important theorem, stated but not proved, concerning the nature of the form $X\xi + Y\eta + Z\zeta$ where the coefficients of ξ, η, ζ are supposed to be the reduced co-ordinates of any derivative to x, y, z. If $U = 0$ is the equation to the cubic in its general form, obviously X, Y, Z are indeterminate, as each may be augmented by an arbitrary multiple of U of suitable degree and order. Consequently, the theorem ought to have been stated in the following form. The co-ordinates X, Y, Z of any such derivative *may be* so expressed that $X\xi + Y\eta + Z\zeta$ shall be a mixed concomitant to U. The fundamental invariantive concomitants to a ternary cubic involving not more than one system of cogredients and a single linear system of contragredients are eleven in number and of the types underwritten :

4 . 0 . 0
6 . 0 . 0
1 . 3 . 0
3 . 3 . 0
8 . 6 . 0
12 . 9 . 0

4 . 4 . 1
5 . 4 . 1
7 . 4 . 1
9 . 7 . 1
11 . 7 . 1

Hence the co-ordinates of every rational derivative in the natural scale to a point on a cubic curve may be expressed as the coefficients of the contragredient variables in a rational integer function of the above eleven quantities linear in the latter five, and such that its degree and orders for the n^{th} grade are $\frac{4(n^2-1)}{3}$; n^2, 1.

The particular forms of X, Y, Z which appertain to the concomitant $X\xi + Y\eta + Z\zeta$, and which may be called the *normal* forms, it may be added, are those which actually arise from the processes of *colligation* and *reduction* described in the excursus. By *colligation* I mean the determination of the *general* analytical connective of x, y, z ; x', y', z' by the same method as that applied at pages 61, 62, to the canonical quadrinomial form of the cubic. The co-ordinates of such connective are absolutely determinate, inasmuch as the equation which each set of co-ordinates must satisfy is of the order 3, whereas the co-ordinates in question are of the second order only in each set of variables (and of course of the first degree in the coefficients of the cubic). By *reduction* I mean that when in the co-ordinates of the general connective for x, y, z ; x', y', z' are substituted the *normal* forms of the co-ordinates for derivatives of the grades μ, $\mu + 3i$, their common factor of the degorder $(12i^2 - 3, 9i^2)$ is to be cast out.

This common factor, it may be noticed, is *always* a covariant of the cubic. When $i = 1$, it is seen *a posteriori* that this is the case, for its value is expressible (see footnote, p. 87) under the form of a known covariant, say Θ (which was obtained by means of using the canonical form of the cubic); that it must be true for all values of i may be deduced from the general algebraical theorem that if in a covariant to any given form, in place of the variables x, y, z be substituted $\frac{d\Omega}{d\xi}$, $\frac{d\Omega}{d\eta}$, $\frac{d\Omega}{d\zeta}$ where Ω is any invariantive concomitant to such form, and ξ, η, ζ are contragredient to x, y, z, the resulting expression will be itself an invariantive concomitant. To obtain now the reducing factor for the connective to P_μ, $P_{\mu+3i}$ (p. 88) it is only necessary to substitute in Θ x_i, y_i, z_i (the normal co-ordinates of the i^{th} derivative) in lieu of x, y, z where $x_i\xi + y_i\eta + z_i\zeta$ is known to be an invariantive concomitant to the cubic. Hence, by the algebraical theorem above stated, the corresponding reducing factor (not containing ξ, η, ζ) is necessarily a covariant to the cubic, as was to be shown.

Again, if $y = 0$, P will be some inflexion J, and the connective to I, J being called K, P_3 will be the connective of J, K, i. e. I, as before; hence z_3 will contain y, and in like manner it will contain x. Also, since in each case P_3 is I, every derivative of P_3 will be I; hence, when $xyz = 0$, $z_{3\nu}$ becomes 0; consequently z_i (if i is a multiple of 3) contains xyz.

Again, if x_i, y_i, z_i are the reduced co-ordinates of P_i, I say that $x_i(y_i^3 - z_i^3)$; $y_i(z_i^3 - x_i^3)$; $z_i(x_i^3 - y_i^3)$ will be the *reduced* co-ordinates of x_{2i}, y_{2i}, z_{2i}.

For, if possible, let two of the above co-ordinates have a common factor F; then, since x_i, y_i, z_i have no common factor, $x_i^3 - y_i^3$, $y_i^3 - z_i^3$ have a common factor, and when $F = 0$, $x_i^3 = y_i^3 = z_i^3$; but $x_i^3 + y_i^3 + z_i^3 + Kx_iy_iz_i = 0$. Hence, unless $x_i^3 = y_i^3 = z_i^3 = 0$, we must have $3 + \sqrt[3]{1}\,K = 0$, but K is arbitrary. Hence, F must be contained in x_i, y_i, z_i contrary to hypothesis.

Although it is a consequence of a general law* that z_i cannot contain z^2, for present purposes it will be sufficient to establish that z_i cannot, for each of two consecutive values of i, contain z^2. Thus, suppose z_{2i-1} and z_{2i} each contained z^2, then, because z_{2i} contains z^2, z_i must do so too; since, otherwise, $x_i^3 - y_i^3$ must contain z. If that is possible, let $z = 0$; then $x_i^3 - y_i^3 = 0$; but P, and therefore P_i, becomes an inflexion, whereas $x_i^3 = y_i^3$ is the necessary and sufficient condition that P_i is a Plückerian point, which is self-contradictory. But since z_i contains z^2, z_{i-1} must also contain z^2, for z_{2i-1} will be contained (see p. 82) in $\frac{1}{z}(x_iy_iz_{i-1}^2 - x_{i-1}y_{i-1}z_i^2)$, and therefore, if z_{i-1} does not contain z^2, z must be contained in x_i or y_i, which is impossible. In like manner, if z^2 is contained in

---

* The law is that $x^i . y^i . z^i \, x y_i z_i$, cannot for any value of i contain a square algebraical factor, just as and *en dernière analyse* for the same general kind of reason that the binomial exponential $(a^i + b^i)$ can contain no such factor.

z_{2i}, z_{2i+1}, it will be contained also in z_i and z_{i+1}. Hence it would be contained eventually in z, which is absurd.

Again, it may be shown that z will be the only common measure to z_{i-1} and z_i. For, if possible, let them have any other common measure F, and let F become zero. Then P_{i-1} and P_i both become points of inflexion belonging to the system previously designated as I, I', I'', and by a collineation process performed on these points alone or combined with I, P may be obtained. Hence P belongs to the same system of inflexions, i. e. $z = 0$. Hence F would be contained in a power of z, contrary to hypothesis.

I will now show that if the two systems of unreduced co-ordinates obtained by the colligation of

$$\left.\begin{matrix} x_{i-1}, & y_{i-1}, & z_{i-1} \\ x_i &, y_i &, z_i \end{matrix}\right\} \text{ and of } \left\{\begin{matrix} y_{i-1}, & x_{i-1}, & z_{i-1} \\ x_i &, y_i &, z_i \end{matrix}\right.$$

be called F, G, H; F', G', H; respectively, the terms F, G, H; F', G', H can have no other measure common to all four than z, or, in other and more precise terms, z is the greatest common measure to the greatest common measures of F, G, H and of F', G', H. For brevity call the two sets of co-ordinates of P_{i-1} and P_i, u, v, w; u', v', w' respectively. Then the unreduced co-ordinates in question will be (p. 82)

$$\left.\begin{aligned} F &= vwu'^2 - v'w'u^2 \\ G &= wuv'^2 - w'u'v^2 \\ H &= uvw'^2 - u'v'w^2 \end{aligned}\right\} \text{ and } \left\{\begin{aligned} uwu'^2 - u'w'v^2 &= F' \\ wvv'^2 - w'v'u^2 &= G' \\ vuw'^2 - v'u'w^2 &= H \end{aligned}\right.$$

into each of which z necessarily enters as a factor, because w, w' have been proved each to contain z.

[u, v, it will be observed, cannot have a common factor, for then u, v, w would have a common factor contrary to hypothesis; and, in like manner, u', v' can have no common factor.]

I say, in the first place, that no indecomposable function of x, y, z, say M, not contained either in w or in w', can be common to F, G, F', G'. For, if so, let F vanish; then, calling $\frac{u}{w}, \frac{v}{w}; \frac{u'}{w'}, \frac{v'}{w'}$, r, s; r', s' respectively, we have

$$\begin{aligned} &(1) \quad sr'^2 - s'r^2 = 0, \qquad && rr'^2 - s's^2 = 0, \quad (3) \\ &(2) \quad rs'^2 - r's^2 = 0, \qquad && r'r^2 - ss'^2 = 0. \quad (4) \end{aligned}$$

Now, none of the terms v, s, r', s' can vanish: e. g. r cannot vanish, for, if so, from (1) it would follow that $s = 0$, or $r' = 0$, and from (3) that $s = 0$, or $s' = 0$, so that either $r = 0$ and $s = 0$, or $r' = 0$ and $s' = 0$, i. e. the general values of u and v or of u' and v' must have a common factor M, which is impossible. Hence, combining (1) and (2) or (3) and (4), we derive $rs = r's'$ (5), as might also be obtained immediately by equating to zero the term common to the two systems above.

From (5), from (3) and (4), and from (1) and (2) we obtain respectively

$$r^3s^3 = r'^3s'^3, \quad r^3r'^3 = s^3s'^3, \quad r'^3s^3 = r^3s'^3,$$

the second and third of which are equivalent to $r^6 = s^6$, $r'^6 = s'^6$, and the first and second combined give $r'^6 = s^6$. Hence $r^6 = r'^6 = s^6 = s'^6$, and consequently the original equations (1), (2), (3) give $r^3 = s^3 = r'^3 = s'^3$.

The equations $r^3 = s^3$, $r'^3 = s'^3$ imply that P_{i-1}, P_i are each of them distinct or identical antitangentials to one of the points of inflexion corresponding to $z = 0$, i. e. are each of them a Plückerian point on the cubic, and P or (P, I) will be a residual either to P_{i-1}, P_i or to $(P_{i-1}, I), P_i$ where I is the auxiliary inflexion used to complete the scale. Hence P is either a Plückerian or an inflexion point, and in either case P_2 will necessarily be an inflexion. Hence one at least of the derivatives P_{i-1}, P_i is an inflexion, but each is a Plückerian, which is absurd.

Thus M (an irresoluble factor common to F, G, F', G') must be contained either in w or in w'. Suppose it is not z and is contained in w, then it cannot be contained in w', for w, w' have no common measure except z, and consequently when $M = 0$, $v'u^2 = 0$, $u'v^2 = 0$, $v'v^2 = 0$, and $u'u^2 = 0$, and either u and v or u' and v' each become zero, which is impossible seeing that neither the general values of u, v nor those of u', v' can have any common factor. In like manner, it follows that M cannot be contained in w'. Consequently, the two systems F, G, H; F', G', H can have no other common measure, except some power of z.

Finally, I say that the only common measure in question is z itself. 1°. Suppose it were possible (which it is not) that one of the two terms w or w' (say w) contains z^2, then it has been proved that the other (w') cannot contain z^2. Hence, if $wvv'^2 - w'u'u^2$ contains z^2, u or u' must contain z, and in like manner, if w' and not w contained z, v or v' must contain z, none of which suppositions are admissible.

2°. Suppose that neither w nor w' contains z^2. Then writing $w = \omega z$, $w' = \omega' z$, and writing for $\frac{u}{\omega}, \frac{v}{\omega}$; $\frac{u'}{\omega'}, \frac{v'}{\omega'}$, r, s; r', s' respectively, we shall obtain over again, as before, $r^3 = s^3$, $r'^3 = s'^3$, indicating as before that P_{i-1} and P_i are each of them Plückerian points when $z = 0$, i. e. when P is a point of inflexion, which is doubly absurd. Hence it follows that the common measures of F, G, H and of F', G', H have the common measure z, and no other.

We are now in a position to prove the *law of squares*. Suppose it is true for P_{i-1} and P_i, I say it will be true for P_{2i-1}. For consider the connectives of

$$\left.\begin{matrix} x_{i-1}, & y_{i-1}, & z_{i-1} \\ x_i\ \ , & y_i\ \ , & z_i \end{matrix}\right\} \text{ and of } \left\{\begin{matrix} y_{i-1}, & x_{i-1}, & z_{i-1} \\ x_i\ \ , & y_i\ \ , & z_i \end{matrix}\right.$$

as expressed by the formulas above employed. Let $z^2\Omega$ be the third term common to the unreduced systems of co-ordinates.

Allowing (as is the fact) that Ω does not contain z, the reducing factor common to the unreduced co-ordinates of P (or it may be its opposite in respect to I) must be $z\Omega$, and consequently to the other system corresponding to P_{2i-1} or its opposite, can only be z or z^2; but the latter is impossible, for then z_{2i-1} would not contain z.

Again, if Ω could be conceived equal to $z^q\Omega_1$, the reducing factor for P or its opposite would be $z^{1+q}\Omega_1$, and consequently that for P_{2i-1} or its opposite could not be z^2 and would be z as before. Hence the order of P_{2i-1} in the variables is necessarily $2(i-1)^2 + 2i^2 - 1$, i. e. $4i^2 - 4i + 1$ or $(2i-1)^2$.

Moreover, it has been shown that if x_i, y_i, z_i are the reduced co-ordinates for P_i, $x_i(y_i^3 - z_i^3), y_i(z_i^3 - x_i^3), 2_i(x_i^3 - y_i^3)$ are such for P_{2i}, and consequently, if the law is true for i, it is true for $2i$. Hence, being true for 1, it is true for 2, and therefore for 3, and therefore for 4 and 5 and 6, and therefore for $3 + 4$, i. e. 7, and for $2 . 4$, i. e. 8, and for $4 + 5$, i. e. 9, and for $2 . 5$, i. e. 10, and so on for every number, as was to be proved.* Thus, this negative proposition, as I have termed it (p. 85), is completely established. There remains to prove the important proposition contained (but incorrectly proved) on pages 84, 85, to wit, that the unreduced systems of co-ordinates arising from the colligation of

$$\left.\begin{matrix} (x_i, y_i, z_i) \\ (x_j, y_j, z_j) \end{matrix}\right\} \text{ and of } \left\{\begin{matrix} (y_i, x_i, z_i) \\ (x_j, y_j, z_j) \end{matrix}\right.$$

will be of the forms LN', MN', NN'; $L'N, M'N, N'N$, where L, M, N; L', M', N' are the reduced systems of the co-ordinates of the connectives of P_i, P_j, and P'_i, P_j respectively.

To illustrate this proposition by an example, consider the connectives of P', P_3, i. e. P_2 and of P, P_3, i. e. P_4.

z_2 is $z(y^3 - x^3)$ and z_4 is of the form $z(y^3 - x^3)\,\Omega$, where Ω is of the order 12 in the variables.

---

* In other words, if the theorem is true up to i inclusive, any number between $i + 1$ and $2i$ inclusive is either of the form $2j$ or $2j - 1$, where j does not exceed i; and being true for j, it is true for $2j$, and being true for $j - 1$ and j, it is true for $2j - 1$. Hence, if true up to i it is true up to $2i$, but it is true for $i = 1$ and therefore for all values of i. Q. E. D.

Call X_4, Y_4, Z_4 the unreduced co-ordinates arising from the colligation of P, P_3. Suppose $x^3 - y^3$ to become zero, then P becomes a Plückerian, and P_3 will be also such, viz. one of the nine appertaining to the inflexions given by $z = 0$.* Hence $x_3^3 - y_3^3$ becomes zero. Now X_4, Y_4 represent $yzx_3^2 - y_3z_3x^2$, $xzy_3^2 - x_3z_3y^2$ respectively, and since $yzx_3^2 \,.\, x_3z_3y^2 - y_3z_3x^2 \,.\, xzy_3^2 = zz_3 (x_3^3y^3 - y_3^3x_3^3) = 0$, $X_4 : Y_4 :: yx_3^2 : xy_3^2$, and consequently $X_4^3 - Y_4^3 = 0$; but P_4 is a point of inflexion and not a Plückerian; hence X_4, Y_4 must each contain the factor $x^3 - y^3$, and Z_4 must be of the form $z^2 (x^3 - y^3)^2\Omega$, for after division by $z (x^3 - y^3)$ it must still contain that factor. Also X_4, Y_4, Z_4 can have no other common measure except $z (x^3 - y^3)$, for after throwing out that factor the quotient is of the order 16, the order of z_4 given by the law of squares. Thus we see that the third unreduced coefficient common to (P, P_3) and (P', P_3) is equal to $z_2 \,.\, z_4$, as it ought to be according to the proposition in question.

To be Continued.

---

* The nine points of inflexion on a cubic curve form a closed group, but so also do any three of them which lie in a right line, and also any single one. In like manner, the nine inflexions with their antitangentials, any three of these lying in a right line with their antitangentials, and any one with its antitangentials, form closed groups containing 36, 12, and 4 points respectively. The ornamental-gardening problem of *alignement*, anglicè *allineation*, which consists in so disposing a number of points on a plane as to obtain the maximum number or all the various possible numbers of right lines each containing three of the points, finds its systematic solution in the theory of groups of inflexional and sub-inflexional points of various grades. In some very old numbers of the "Educational Times" will be found questions of the kind proposed by me (not reproduced in the Reprint), of which the solution depends on this order of considerations. In certain cases that had been studied, I ascertained the possible existence of a larger number of collineations than had previously been imagined by other writers on the subject, among whom Mr. S. B. Woolhouse deserves special mention for the ingenuity of his constructions. As far as I am aware, the theory of allineation has never been treated by other writers than myself, except by empirical methods, and its dependence on the theory of the general cubic curve was not even suspected.